CYBERWOMEN

Online violence against women

Online violence against women

https://iwpr.net/

Contents

Spectogram

- **Objective(s):** To provide a useful way for participants to know each other's thoughts on specific issues, by creating a live spectrum of opinion in the training space.
- **Length:** 90 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - A feminist internet[1]
- **Needed materials:**
  - A large room or outdoor space
  - Yourself!

The content for this exercise was developed by Mariel Garcia (SocialTIC) and Spyros Monastiriotis (Tactical Technology Collective)

[1] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

Leading the session

1. Begin by indicating for the group where the two ends of the Spectrogram "spectrum" are located – if using an indoor space, these can be opposite ends of a room; for an outdoor space, it could be two trees, walls or other points.
2. Explain that each of the two ends represents a general opinion – indicate that one end will represent "Strongly Agree" and the other will represent "Strongly Disagree".
3. Now, explain how the exercise will work – you will read out a statement (it is important that these be phrased as statements and not questions), and then repeat it; then, participants will arrange themselves along the "Strongly Agree – Strongly Disagree" spectrum in a way that represents how strongly they feel about the statement you've just read.
4. Remind participants that they don't need to choose only one end of the spectrum or the other; they can stand at the exact middle point if they are undecided on their opinion, or they can stand along any other point that indicates the extent to which they Agree or Disagree with the statement.
5. In this Spectrogram, you will be reading aloud several statements related to digital security and women's online experiences – here below are examples of statements you can use:
    - There is no good reason for anyone to share their email/social networks password.
    - Sometimes it is necessary for us as women to avoid sharing certain opinions online.
    - Women and men activists face the same type of violence and threats online.
    - My work becomes impossible without safe access to online spaces.

6. After participants have arranged themselves following a statement, ask 2-3 participants why they chose to stand where they are, as this can make for interesting discussions.
7. You can also tell participants that if, after hearing someone's explanation, they decide that they've changed their opinion, they can move to a different spot on the spectrum if they want – be sure to ask why they decided to move!

A feminist internet

- **Objective(s):** To provide an awareness raising opportunity for participants about the challenges faced by women in online spaces.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Her-story of technology[1]
  - Symbolic violence[2]
- **Needed materials:**
  - Flipchart paper
  - Colored Markers
  - Copies of Feminist Principles of the Internet[3] for participants

[1] https://cyber-women.com/en/rethinking-our-relationship-with-technology/herstory-of-technology/

[2] https://cyber-women.com/en/online-violence-against-women/symbolic-violence/

[3] http://feministinternet.net

Leading the session

Part 1 – Raising Awareness

1. Start the session by asking participants - What some common messages or ideas they have heard about women and technology? What are the prevailing attitudes regarding women and technology in their country(ies)?
2. Ask participants to brainstorm some of the obstacles that women often face while trying to access and use technology, or participate actively in online spaces. They can do this all together, or in small groups – the choice is yours. Write down the obstacles that the group comes up with on a large sheet of flipchart paper.
3. Once the brainstorming and discussion has completed, share some of the following global statistics with participants - if possible, also try to include specific country or region-focused statistics relevant to the context of participants:
    - Internet penetration rates are higher for men than for women in all regions of the world - the global Internet user gender gap is 12%.
    - 60% of the cases of technology-related violence against women were not investigated by authorities.
    - Of all the Wikipedia editors online globally, between 84 and 91% percent of them are male.
    - Women occupy 27% of the top management jobs in media companies and 35% of the workforce in newsrooms.
    - Women in tech are paid at least 28 percent less than men with the same education, years of experience and age.
4. Divide participants into small groups and ask them to reflect on the data shared - What are the implications of these statistics for the lives of women, and for shaping the Internet as a common space for all of us to inhabit freely?

Part 2 - Feminist Principles of the Internet

5. Now introduce APC's Feminist Principles of Internet, as an exercise to reflect on what is needed to build:

   > [...] a feminist internet that works towards empowering more women and queer persons to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy.

6. Give each of the groups a set of the Feminist Principles of the Internet – this can be the actual document itself (downloaded from the site) or a handout with the text of the principles, which are divided into the categories of:

   - Access
   - Movements and Public Participation
   - Economy
   - Expression
   - Agency

7. Ask each group to discuss how each of the principles applies to their own context, and to make a list of ways in which each participant can contribute to changing that reality of women and technology.

8. Ask each group to present the principles they reflected on and their conclusions.

References

- http://feministinternet.net
- https://en.wikipedia.org/wiki/Gender_bias_on_Wikipedia
- http://cdn.agilitycms.com/who-makes-the-news/Imported/reports_2015/global/gmmp_global_report_en.pdf

Symbolic violence

- **Objective(s):** Demonstrate for participants how to identify symbolic violence, and how to draw connections between symbolic violence and online gender-based violence.
- **Length:** 30-45 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Spectrogram[1]
  - A feminist internet[2]
- **Needed materials:**
  - Flip charts
  - Pens or pencils
  - Colored sheets
  - Post-It Notes
  - Adhesive Tape

[1] https://cyber-women.com/en/online-violence-against-women/spectrogram/
[2] https://cyber-women.com/en/online-violence-against-women/a-feminist-internet/

Leading the exercise

Part 1 - What is Symbolic Violence?

1. Begin with an explanation of what is meant by the term 'symbolic violence':

   > Symbolic violence is inflicted through impositions of gendered cultural norms and behaviors. Women are taught that "something" might happen to us if we decide to walk alone at night, dress a certain way, or act carelessly: fear becomes a normalized and accepted mental state.
   >
   > This means that we, as women, are held responsible for any violence we might face, which in turn creates fear or even terror – this fear or terror generates a "mental map of forbidden spaces" for us, eliciting conditioned responses such as:
   >
   > Feeling the need to return home at night in a taxi or with a companion; Walking more quickly or even running if we hear footsteps behind us; Unconsciously practicing self-censorship on social media and other online platforms; Deciding not to go out, or to dress a certain way, for fear of what may happen to us;
   >
   > Furthermore, though women are made to feel responsible for the violence we experience, at the same time we are never provided strategies and resources to address that violence (aside from the conditioned responses above), nor to enjoy and occupy spaces, or to be free in our movement and speech and with our body and sexualities, etc.
   >
   > Symbolic violence creates prohibited spaces and situations for women, thereby denying us our fundamental right to security and free movement; compounding this problem is the impunity often granted to our aggressors – often, they

are not questioned but rather pathologized as "crazy" or inherently unable to take control of or responsibility for their actions.

At this point, you may also want to discuss images of violence against women (symbolic or otherwise) which are disseminated and normalized through the media, and especially in online spaces.

Part 2 - Identifying Symbolic Violence for Ourselves

2. Hand out to each participant a small stack of post-it notes, on which they should identify and write down examples of activities they have stopped doing, or behaviors they have modified, because of the symbolic violence they experience as women occupying offline and online spaces. Once finished, gather the post-its and read aloud some of the examples shared – discuss these together as a group, commenting on possible motivations for changing these behaviors and perceived fears.
3. Immediately following the group discussion, explain that there are three main factors which construct and enable fear and terror in response to symbolic violence:
    - **Appropriation of the Female Body:** the female body is still seen as an object for male enjoyment, bring about a lack of security or confidence in the body's own resources and capacities.
    - **Guilt and Shame:** these are both seen as permanent, unshakeable elements that facilitate the perception of perpetrated gender-based violence as deserved or somehow acceptable.
    - **"Learned Helplessness":** this is a psychological state that occurs frequently when events are seen to be uncontrollable – when the perception is that there is nothing that can be done to change the outcome of an action, the mental state adjusts accordingly by sacrificing its agency to assert any control over that outcome (instead, accepting and normalizing it).

4. After explaining these three factors, ask participants what strategies they can think of to transform these factors into approaches for tackling symbolic violence! Have them write these down on their post-it notes. Below are some possible strategies that could be proposed:

    - Regaining control of your body's narrative, defining and asserting it as a territory of both pleasure and resistance.
    - Recognize and accept the damage which has been done to your body (physically or mentally), moving past any self-perception as a victim and instead building up the resilience of a survivor.
    - Build and sustain networks of support for yourself and others, both online and offline. We are never alone in this struggle.

References

- https://en.wikipedia.org/wiki/Learned_helplessness
- http://www.autodefensafeminista.com/attachments/article/277/MANUAL%20Autodefensa%20Feminista.pdf

Reporting abuse on social media platforms

- **Objective(s):** To share with participants some tips for denouncing online violence in social media platforms like facebook and twitter.
- **Length:** 40 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Safe online campaigning[1]
  - Apps and online platforms: friend or foe?[2]
  - Let's start a documentation journal!
- **Needed materials:**
  - Projector and slides
  - Post its
  - Computer for every two participants (if possible)

[1] https://cyber-women.com/en/safe-online-advocacy/safe-online-campaigns/
[2] https://cyber-women.com/en/privacy/apps-and-online-platforms-friend-or-foe/

- **Recommendations:** This session is highly recommended for groups of women who have being harassed online or who are involved in online campaigning.

Leading the session

1. Start the session by asking participants:
    - Do they know of any women's collectives or women activists who have been harassed online?
    - If so, on which platform(s) did it happened?

    Ask them to offer examples of tactics they have seen used by those groups or individuals to address or counter online harassment, or tactics that they themselves have used. Have participants write these on post-it notes.
2. Share some recommendations of basic practices for denouncing online violence against women that are commonly used, as well as any NGOs or collectives that can provide assistance in response to such harassment:
    - Facebook recommends flagging the exact comment or post, providing as much context as possible in the reporting process. Participants can check updates to this process here: https://www.facebook.com/report
    - Blocking harassers will prevent them from sending friend/follow requests, starting a conversation or sending any messages, and seeing any updates posted to a user's feed. Users are not notified when they've been blocked, but they may still notice that it has happened if they are suddenly no longer able to contact a target.
    - Take screenshots before blocking harassers on platforms to keep as documented evidence of abuse – once they are blocked, it becomes much more difficult to collect supporting evidence, which users may be asked to offer during an investigation into the incident (you may want to show participants how to take screenshots

on their computers if they don't know to do so already)
- Twitter recommends that users who are the target of online harassment report the incident and keep a record of the case number for any follow up action. On Twitter it is possible to report an individual tweet as well as an entire profile.

It is recommended to avoid clicking on any links that may be received in messages or other communication sent by harassers, as they could potentially lead to malware being installed on a user's device.

3. During this part of the session, you should also demonstrate to participants how they can block users and report profiles or posts on Facebook and Twitter, in addition to any other social media platforms that they frequently use. Make sure to research these before the training so you are up to date, as these processes unfortunately tend to change quite frequently (as do account privacy settings).
4. If you would like to offer participants an opportunity for some hands-on practice, have them break off into small groups and look for pages or profiles that may be targets of online abuse or harassment - for example, they should try out documenting any posts or profiles on Facebook that are actively perpetrating such harassment, and then filing reports using the established process.

References

- https://karisma.org.co/descargar/manualseguridadtw

Let's start a documentation journal!

- **Objective(s):** To introduce participants to more in-depth practices related to reporting abuse online, specifically documentation of incidents.
- **Length:** 45 minutes
- **Format:** Session
- **Skill level:** Basic
- **Required knowledge:**
  - None required
- **Related sessions/exercises:**
  - Reporting abuse on social media platforms[1]
  - Doxxing the troll[2]
- **Needed materials:**
  - Slides (with key points included below)
  - Laptop/Computer and Projector setup

[1] https://cyber-women.com/en/online-violence-against-women/reporting-abuse-on-social-media-platforms/

[2] https://cyber-women.com/en/online-violence-against-women/doxxing-the-troll/

  - Printed copies of Documentation Journal templates (see below)
- **Recommendations:** This session is recommended when working with groups that deal with online harassment, those who have received threats online and offline, or those who will be working on projects or campaigns that could elevate their risk of exposure to harassment.

Leading the session

Part 1 - Why is Documentation Important?

1. In this first part of the session, you will begin by explaining the following to participants:

   What is Documentation?

   Documentation in this context refers to a systematic, organized approach for keeping a track of any incidents of abuse or harassment that occur in the course of our work – essentially, it is maintaining an archive of evidence.

   What is an Incident?

   An incident is anything that happens either online or offline that might constitute abuse or harassment – whether an event can be classified as an incident or not is highly dependent on the context and circumstances in which it happens, and the severity of its impact in relation to those. For example, if you receive an email that seems like a phishing attempt – and you're used to receiving these every so often – that alone might not be significant enough to be an incident; however, if your organization is about to launch a major campaign, and you begin receiving an unusually large number of these emails, this would likely constitute an incident (and it should be documented). To provide another example, the same could be said if your organization is about to launch a major campaign and you begin receiving usually large numbers of Facebook friend requests from strangers.

What is a Documentation Journal?

A documentation journal is a place where you can keep records of incidents that occur, in an organized way that will help you save important information and evidence from each for later use or reference.

Why is Documentation Important?

Documentation can be useful for later reference when attempting to connect the dots between different incidents that took place during a specific timeframe, or that happened to several people in the same organization. Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for identifying adversaries, or to draw connections between certain kinds of incidents and certain actions of yours or your organizations. When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.

Part 2 – How Can We Document Incidents?

2. Once you've finished reviewing the above points about documentation and why it is important, you can hand out to participants printed copies of the below Documentation Journal templates.
3. Mention to participants that these templates provide just one example of the kinds of information that could be important to gather when documenting incidents. They should feel free to add or remove columns and fields as they see fit when creating more specific formats contextualized to their work in the future.

There are two templates included here – one for documenting online incidents, and another for physical/offline incidents (begins next page):

Documentation Journal Template (Online)

Date
Time
Summary of incident
Platform
URL
Screenshot (filename or copy/pasted)
Description of screenshot content(s)
Risk level
Follow-up actions
Notes

Documentation Journal Template (Offline/Physical)

Date
Time
Location
Summary of incident
People involved
Risk level
Follow-up actions
Notes

4. Most of the fields in these templates are relatively self-explanatory; however, you should still walkthrough each one for the group, describing briefly to what each one refers (in terms of what participants should be keeping track of for each).
5. Be sure to specifically highlight the **Level of Risk** field, as this field is highly subjective and less self-explanatory than the others. How different participants and/or organizations define levels of risk will be

extremely specific to their context – it might be useful to pause at this point and ask participants for examples of incidents they would define as Low Risk, Medium Risk, or High Risk (for instance). Emphasize to participants that they should consider the potential **impact** of the incident (on either a personal or organizational level, or both) when defining risk in this context.

Optional: Either before or immediately following this session, go through the Gender-Based Risk Model exercise with participants. During that exercise, the group will have a more focused opportunity to define levels of risk for their own context – they can then apply those definitions of risk to their documentation journals.

6. Finally, another important field to highlight during this part of the session is **Follow-up Actions**. Essentially, a Follow-up Action is the next step that will be taken to address the current incident (such as filing a report on Facebook), or a measure that will be implemented to prevent the incident from happening again or to reduce its impact.

   Optional: Either before or immediately following this session, go through the Organizational Security Plans and Protocols session with participants. During that exercise, the group will have a more focused opportunity to define security plans and protocols in response to certain known or potential risks – similar steps would be required when planning Follow-up Actions for incidents.

Part 3 – Starting Our Documentation Journals

7. Ask participants to begin filling in their journal templates individually - give 10-15 minutes to fill in as much as they can. Although they can fill in the details of actual incidents that have occurred if they wish, participants can also use hypothetical examples for practice purposes.
8. Once they finish their first draft of the journal, ask them to get together in pairs and share the incidents they've recorded with their partner – for this step, pairing together participants from the same organization

(if applicable) will be helpful. Each pair should ask questions of each other about the level of detail or thoroughness in their incident reports – in some cases, this may help a participant recall specific details they may not have remembered earlier. Note that **some participants might not feel comfortable sharing their journal with others**, so allow them to work individually if they so choose.

Part 4 - Practices and Tips for Maintaining Documentation Journals

9. Remind participants that, to keep up regular maintenance of their documentation journals, they will need to find ways to "socialize" (or integrate) journal updating into existing routines. In the context of an organization, participants should think about whether there will be a specific person in charge of gathering information for the journal; alternatively, it may be easier or more agreeable to rotate the task among individuals or among teams. You should also mention here that it may be good idea, if someone within the organization is the subject of an incident, for someone other than themselves to document the incident.
10. Encourage participants to experiment with different workflows to make updating their documentation journals a more efficient process – there may be ways of automating certain processes, or they may find that certain fields in the templates included above are irrelevant for their context (which will save them unnecessary work.
11. Close the session by asking participants, now that they've had time to think about the importance of documenting incidents for their own contexts, if they have any key takeaways from the discussion or ideas to make journal maintenance and updating an easier process.

Doxxing the troll

- **Objective(s):** To introduce participants into a series of tools and activities focused on gathering information about their online harassers. this information can be used to help them make decisions in terms of privacy and security online.
- **Length:** 180 minutes
- **Format:** Exercise
- **Skill level:** Basic
- **Required knowledge:**
  - Basic digital security concepts and/or previous training
  - Safe browsing[1]
  - What does your metadata say about you?[2]
- **Related sessions/exercises:**
  - Safe browsing[3]
  - What does your metadata say about you?[4]

[1] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

[2] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

[3] https://cyber-women.com/en/digital-security-basics-1/safe-browsing/

[4] https://cyber-women.com/en/safe-online-advocacy/what-does-your-metadata-say-about-you/

    - Let's start a documentation journal!
- **Needed materials:**
    - Printed copies of the Documentation Journal Template (Online)
    - Slides (with key points included below)
    - Laptop/Computer and Projector setup
- **Recommendations:** This exercise is recommended for groups of whrds that are currently experiencing online harassment/online threats, or those who have very recently experienced these. though not explicitly required, this exercise works best if participants have already done let's start a documentation journal! this exercise works best if participants each have their own device or computer. you may want to split this session into two parts, as it is quite long and can be very intensive – you can also keep this as one session, but with a longer than normal break in the middle.

This exercise was adapted from an activity developed by Indira Cornelio (SocialTIC) and Phi Requiem (#SeguridadDigital) with the collaboration and support of APC's Take Back the Tech

Leading the exercise

Part 1 – What is Doxxing?

1. Explain to participants what Doxxing means – essentially, it's the practice of gathering a substantial amount of personal information about someone and then making it public (usually online). You should also explain how doxxing is sometimes used against people as a revenge tactic, and is often used to endanger, harass, or threaten activists and human rights defenders.
2. Highlight this important reminder for participants before continuing onward with the exercise:

   The goal of this exercise is not to recommend doxxing as a best practice (or to recommend using illegal or dubious methods of doing so) –

as doxxing implies the public release of personal information, it is important to highlight that 'outing' someone's identity or information is not necessary. Rather, the goal of this session is to show participants how to gather this kind of information online to help them make informed decisions about addressing abuse or harassment.

3. Finally, explain also that it is important for participants to recall what they know about safe browsing practices – part of this exercise involved visiting harasser's profiles and online spaces.

Part 2 – Identifying Harassers

4. Work with participants to set their expectations for the exercise, asking them - What do they want to find out about their harasser(s)? Mention several possible motives before participants begin sharing:
    - Is it to know their real identity?
    - To understand their motives for harassing them?
    - To find out if they are harassing other WHRDs as well?
    - To find out if it is just one person, or several people acting as one?
5. You may find that some participants have heard of ways to obtain this kind of information about their harassers, but make it clear to them that the tools and tactics you will be sharing have certain limitations. If the group has already done the Let's Start a Documentation Journal! session, remind them of the importance of maintaining that body of evidence – it is critical for establishing patterns of abuse and for reporting harassment. If the group has not already done the Let's Start a Documentation Journal! session, explain that later in this exercise you will review a method for keeping track of harassment incidents.

Part 3 - Different Profiles, Different Motives

6. Share a couple of cases of women activists or journalists and their experiences with online harassment. Try to find cases that are relevant

to the context of the participants, and that show different profiles of harassers and different motives for their actions.

7. Only if there are any women who feel comfortable sharing their own experiences with online harassment, ask them – About when did it begin? Who do they think the harasser is? Do they know them? Is there a specific motivation they can think of for their actions?
8. Reflect on possible motives that their harasser might have - Is the harassment happening because they are a women? Because they defend women's rights/human rights? Have they seen this kind of harassment against their male partners or colleagues? If so, does it happen the same way or differently?

Part 4 - Documenting Incidents & Threats

9. If participants have already gone through the Let's Start a Documentation Journal! session, review the key takeaways with participants once more and explain how a documentation practice is an important part of gathering information about harassers to make decisions about next steps and actions. You can then skip down to Part 5 – Getting Ready.
10. If participants have not yet gone through the Let's Start a Documentation Journal! session, start out by first explaining the following points, which highlight why documentation is an important practice for addressing online harassment:

    What is Documentation?

    Documentation in this context refers to a systematic, organized approach for keeping a track of any incidents of abuse or harassment that occur in the course of our work – essentially, it is maintaining an archive of evidence.

    What is an Incident?

    An incident is anything that happens either online or offline that might constitute abuse or harassment – whether an event can be classified

as an incident or not is highly dependent on the context and circumstances in which it happens, and the severity of its impact in relation to those. For example, if you receive an email that seems like a phishing attempt – and you're used to receiving these every so often – that alone might not be significant enough to be an incident; however, if your organization is about to launch a major campaign, and you begin receiving an unusually large number of these emails, this would likely constitute an incident (and it should be documented). To provide another example, the same could be said if your organization is about to launch a major campaign and you begin receiving usually large numbers of Facebook friend requests from strangers.

What is a Documentation Journal?

A documentation journal is a place where you can keep records of incidents that occur, in an organized way that will help you save important information and evidence from each for later use or reference.

Why is Documentation Important?

Documentation can be useful for later reference when attempting to connect the dots between different incidents that took place during a specific timeframe, or that happened to several people in the same organization. Documentation can reveal patterns of abuse or other online attacks you may not have otherwise noticed, by presenting a collated body of evidence – these patterns can be helpful for identifying adversaries, or to draw connections between certain kinds of incidents and certain actions of yours or your organizations. When reporting incidents of abuse on social media platforms, for instance, evidence such as screenshots or profile names may be requested during an investigation.

11. Now, you can introduce the Documentation Journal to participants – for this exercise, you can just use the Online version, which you should have printed versions of prepared to hand out to the group – see the template below:

Documentation Journal Template (Online)

Date
Time
Summary of incident
Platform
URL
Screenshot (filename or copy/pasted)
Description of screenshot content(s)
Risk level
Follow-up actions
Notes

12. Mention to participants that this template provides just one example of the kinds of information that could be important to gather when gathering information about harassers. They should feel free to add or remove columns and fields as they see fit when creating more specific formats that are relevant to their context.
13. Most of the fields in these templates are relatively self-explanatory; however, you should still walkthrough each one for the group, describing briefly to what each one refers (in terms of what participants should be keeping track of for each).
14. Be sure to specifically highlight the Level of Risk field, as this field is highly subjective and less self-explanatory than the others. How different participants and/or organizations define levels of risk will be extremely specific to their context – it might be useful to pause at this point and ask participants for examples of incidents they would define as Low Risk, Medium Risk, or High Risk (for instance). Emphasize to participants that they should consider the potential impact of the incident (on either a personal or organizational level, or both) when defining risk in this context.
15. Ask participants to begin filling in their journal templates individually

- give 10-15 minutes to fill in as much as they can. Although they can fill in the details of actual incidents that have occurred if they wish, participants can also use hypothetical examples for practice purposes.

Part 5 – Getting Ready

16. Before moving on to the next steps in the exercise, for participants to be careful not to click on any link they might receive or find while doxxing their harasser – these could be possible phishing attempts (explain what this is if participants are not familiar) that could install malicious software on their devices. Highlight that its extremely important to avoid providing additional information about yourself to harassers; likewise, for participants going through this exercise who are not currently experiencing online harassment, they will want to avoid attracting unnecessary attention to themselves that could lead to later harassment:
17. Walk participants through the following steps to safely begin gathering information about their harassers:
    - They should collect any information they may already have on hand about their harassers (or document any past incidents they can recall in their documentation journals);
    - Then, they should choose the browser they will use for their investigation – on that browser, they should logout from any of their accounts, and erase their browsing history and cookies. They may want to consider using Tor Browser for this activity, if you have already covered this with them;
    - They may also want to consider creating new online identities or profiles to perform this activity (such as an alias Facebook or Twitter account, or a fake Gmail account) – remind them to be careful not to use any information for these accounts that could be used to link back to their real identities!

- Emphasize the importance of taking notes during this process – remind the group of what you discussed when addressing the importance of documentation practices.
- Have participants create a dedicated folder on their computers to gather and store any information or evidence they collect – these could be avatar images, screenshots, user names, email and social media accounts, comments on forums, or mentions of their possible locations or other known contacts.

Part 7 – Useful Tools

18. Now you can start sharing examples of tools that will be useful to participants during their doxxing investigation - if possible, provide participants a copy of your presentation containing this information, or a handout with the tool list and links that they can refer to later on their own.
19. Explain each of the tools, giving participants a few minutes for each to locate them online and try them out (aside from those included here, feel free to add any others you know of that could be useful or relevant):
    - Google searching, or Duck Duck Go[5];
    - Advanced search on Twitter[6];
    - Checking Whois.net in case they can find information that comes from a website to see if there is any information about who owns the domain;
    - Google reverse image search[7] in case they have received images or photos they can do an image search;
    - Metadata tools in case they have received images or photos they can see if there is any metadata available:

[5] https://duckduckgo.com
[6] https://twitter.com/search-advanced
[7] https://images.google.com/

- MetaShield[8]
- MetaPicz[9]
- Social Mention[10];
- Follower Wonk[11];
- NameCheck[12];

20. Explain also that there are ways for participants to build mini-monitoring systems for tracking information online: this works well for tracking certain profile name, username or hashtag:

    - IFTTT[13] – for IFTTT, explain how it allows users to connect Twitter with Google Drive to keep track of tweets and mentions connected to a certain username or hashtag.
    - Google Alerts[14]
    - Tweetdeck[15]

21. Depending on how much time you have available, participants can either do their investigations now during the workshop, or they can do them as "homework" for the next training day. Either way, remind the group that it will be helpful – once they are done collecting information – to take a step back and look at everything they have gathered:

    - Do they see any patterns emerging?
    - What does the information they have tell them about who their harasser might be?
    - Perhaps they can even predict potential future targets or kinds of attacks?

[8] https://www.elevenpaths.com/technology/metashield/index.html
[9] http://metapicz.com/
[10] http://socialmention.com
[11] https://moz.com/followerwonk/
[12] https://namechk.com
[13] https://ifttt.com
[14] https://www.google.com/alerts
[15] https://tweetdeck.twitter.com

References

- https://summit2015.globalvoices.org/2015/02/do-we-feed-the-trolls-learning-from-our-community/
- https://citizenevidence.org/category/how-to-2/tutorials/